POISSON TYPE PHENOMENA FOR POINTS ON HYPERELLIPTIC CURVES MODULO p

KIT-HO MAK AND ALEXANDRU ZAHARESCU

Abstract. Let p be a large prime, and let C be a hyperelliptic curve over $\mathbb{F}_p$. We study the distribution of the x-coordinates in short intervals when the y-coordinates lie in a prescribed interval, and the distribution of the distance between consecutive x-coordinates with the same property. Next, let $g(P, P_0)$ be a rational function of two points on C. We study the distribution of the above distances with an extra condition that $g(P_i, P_{i+1})$ lies in a prescribed interval, for any consecutive points P_i, P_{i+1}.

1. Introduction

Let p be a large prime. In [3], Cobeli and one of the authors considered the distribution of r-tuples of primitive roots modulo p. They showed that the distribution of primitive roots becomes Poissonian as p tends to infinity via a sequence of primes such that $\varphi(p-1)/p \to 0$. Moreover, they showed that the proportion of distances between consecutive primitive roots which are at least λ times larger than the average value $p/\varphi(p-1)$ tends to $e^{-\lambda}$. In this paper, we employ an analogous technique to study r-tuples of x-coordinates on a hyperelliptic curve modulo a large prime number p.

Let C be a hyperelliptic curve over $\mathbb{F}_p$ defined by the equation $y^2 = f(x)$, f not a square. Let $\mathcal{I}$ be an interval inside $[0, (p-1)/2]$ with $|\mathcal{I}| \geq p/\log\log p$, $|\mathcal{I}| = o(p)$. We consider the x-coordinates of the points $(x, y) \in C$ with $y \in \mathcal{I}$, and denote them $0 \leq x_1 < \cdots < x_m \leq p-1$. We study the distribution of the number of such x_i's in $(x, x+t]$, where x itself is one of such x_i's, and $t \sim \lambda p/|\mathcal{I}|$. It turns out that under certain natural assumptions, as p increases, the distribution approaches the Poisson distribution with parameter λ.

Next, we consider the proportion of distances between consecutive x_i's which are at least λ times greater than the asymptotic average $p/|\mathcal{I}|$, that is,

$$\mu(\lambda) = \frac{\#\{i : 1 \leq i \leq m, x_{i+1} - x_i \geq \lambda p/|\mathcal{I}|\}}{m}$$

where m is the total number of such x_i, and $x_{m+1} = x_1 + p$. As p tends to infinity, we show that the limit of $\mu_p(\lambda)$ tends to $e^{-\lambda}$, and moreover, that this convergence is uniform on compact subsets of $[0, \infty)$.

Lastly, we go a step further and investigate to what extent the above Poisson distribution might be distorted via a rational function $g(P, P_0)$ of two points P, P_0 on the curve C. This builds on, and extends some ideas from [14]. More precisely, we study the distribution of the number of x_i's in $(x, x+t]$ as above, but with the

2000 *Mathematics Subject Classification.* Primary 11G20; Secondary 11T99.

Key words and phrases. Poisson distribution, hyperelliptic curves.

The second author is supported by NSF grant number DMS - 0901621.

extra condition that $g(P_i, P_{i+1}) \in \mathcal{J}$, where $\mathcal{J} = [\alpha p, \beta p)$, and $P_i = (x_i, y_i), P_{i+1} = (x_{i+1}, y_{i+1})$ are points on C with $y_i, y_{i+1} \in \mathcal{I}$. The resulting distribution is again Poisson, but with a different parameter $\lambda' = \lambda(\beta - \alpha)$. Regarding the proportion of distances between consecutive x_i's satisfying the above extra condition, that is,

$$\mu(\lambda, \alpha, \beta) = \frac{\#\{i : 1 \leq i \leq m, x_{i+1} - x_i \geq \lambda p / |\mathcal{I}|, g(P_i, P_{i+1}) \in [\alpha p, \beta p]\}}{m}, \tag{1.1}$$

we show that as p tends to infinity, $\mu_p(\lambda, \alpha, \beta)$ tends to $e^{-\lambda(\beta-\alpha)}$.

As an application of our results, we will derive a result which shows how the distribution of distances between the x-coordinates of points on an elliptic curve C is affected by the group law of C. This is our original motivation for studying this problem.

2. Distribution of Values of Rational Maps on an affine curve in a hypercube modulo p

Since the Poisson distribution of x-coordinates in short intervals without any distortion g and its corresponding limit distribution of consecutive difference can be derived from the case with distortion by simply setting $\mathcal{J} = [0, p)$, i.e. $\alpha = 0, \beta = 1$, we will proceed directly to prove the results when distortion exists, and derive the case without distortion as a corollary.

Let p be a large prime number, and let X be an irreducible affine curve over $\mathbb{A}_p^r$, the affine r-space over $\mathbb{F}_p$, given by the set of equations $f_i(\boldsymbol{x}) = 0$, where $\boldsymbol{x} = (x_1, \ldots, x_r)$, $1 \leq i \leq k$. By the well known Weil bounds for space curves [1] (note that in our case X is affine instead of projective) we know that

$$|\#X - p| \leq 2g_a\sqrt{p}, \tag{2.1}$$

where g_a denotes the arithmetic genus of X. Note that this formula works even when X is singular.

Let $\boldsymbol{g} = (g_1, \ldots, g_s)$ be a rational map from X to $\mathbb{A}_p^s$. Thus each g_i is a quotient of polynomials in $\mathbb{F}_p[x_1, \ldots, x_r]$. Recall that the degree $\deg(g_i)$ of g_i is defined as the maximum between the degree of its numerator and the degree of its denominator. Define the degree of the rational map $\boldsymbol{g}$ to be $\deg(\boldsymbol{g}) := \max_{1 \leq i \leq s} \deg(g_i)$.

For the convenience of the reader, we recall the notion of linear independence on a curve X. A set of functions $\{g_1, \ldots, g_s\}$ is linearly independent provided that if $c_1, \ldots, c_s \in \overline{\mathbb{F}_p}$ are such that $c_1 g_1(\boldsymbol{x}) + \cdots + c_s g_s(\boldsymbol{x}) = 0$ on the curve X, then $c_1 = \cdots = c_s = 0$.

Let $\mathcal{I}_1, \ldots, \mathcal{I}_r$ be intervals in $[0, p)$, and we view $\mathcal{I}_1 \times \cdots \times \mathcal{I}_r \subset \mathbb{A}^r$ as a hypercube in the domain for which X is defined. Similarly, let $\mathcal{J}_1, \ldots, \mathcal{J}_s$ be intervals in $[0, p)$, and view $\mathcal{J}_1 \times \cdots \times \mathcal{J}_s \subset \mathbb{A}^s$ as a hypercube in the range of the rational map $\boldsymbol{g} = (g_1, \ldots, g_s)$. We define

$$\mathcal{N}(X) = \#\{\boldsymbol{x} \in X \cap (\mathcal{I}_1 \times \cdots \times \mathcal{I}_r) | \boldsymbol{x} \text{ is not a pole of } \boldsymbol{g}, \boldsymbol{g}(\boldsymbol{x}) \in \mathcal{J}_1 \times \cdots \times \mathcal{J}_s\}$$

to be the number of points on X lying inside the hypercube $\mathcal{I}_1 \times \cdots \times \mathcal{I}_r$, whose images under $\boldsymbol{g}$ lie inside the hypercube $\mathcal{J}_1 \times \cdots \times \mathcal{J}_s$. The main result of this section is the following theorem, which may be regarded as a uniform distribution result, where the intervals $\mathcal{I}_i, \mathcal{J}_j$ are not too small.

Theorem 2.1. *Let X be as above, of degree $d > 1$, and let $|\mathcal{I}|$ denote the number of integers inside the interval $\mathcal{I}$. Let $\boldsymbol{g} = (g_1, \ldots, g_s)$ be a rational map with*

$1 \le \deg \boldsymbol{g} < d$. *Let p be a large prime, and assume that the set of functions $\{1, x_1, \dots, x_r, g_1(\boldsymbol{x}), \dots, g_s(\boldsymbol{x})\}$ is linearly independent on X. Then*

$$\left| \mathcal{N}(X) - \frac{|\mathcal{I}_1| \dots |\mathcal{I}_r|\, |\mathcal{J}_1| \dots |\mathcal{J}_s|}{p^{r+s-1}} \right| \le 2^{r+s} d(d-1) \sqrt{p} \log^{r+s} p + O(\sqrt{p} \log^{r+s-1} p).$$

Remark 2.2. The uniform distribution problem of rational points over an irreducible variety in a hypercube was investigated by Myerson [10], and also Fujiwara [6] (see also [4] for the case of curves, but with more general regions). Their results were improved in the case for complete intersections by Shparlinski and Skorobogatov [11], Skorobogatov [13] and Luo [8]. On the other hand, the uniform distribution problem of rational maps was investigated by Vajaitu and one of the authors [14] (see also [15] and [7] for other related distribution problems). Here, we combine both ideas, and at the same time produce an explicit error term for later use.

The first step in the proof of Theorem 2.1 is to rewrite $\mathcal{N}(X)$ as an exponential sum.

Lemma 2.3. *Denote $e_p(y) = e^{2\pi i y/p}$, and let $T = \{(t_1, \dots, t_r) : |t_j| \le (p-1)/2\}$ and $U = \{(u_1, \dots, u_s) : |u_j| \le (p-1)/2\}$. We have*

$$\begin{aligned} \mathcal{N}(X) = \frac{1}{p^{r+s}} & \sum_{(t_1,\dots,t_r)\in T} \prod_{1\le i\le r} \left(\sum_{m_i \in \mathcal{I}_i} e_p(t_i m_i) \right) \\ & \times \sum_{(u_1,\dots,u_s)\in U} \prod_{1\le j\le s} \left(\sum_{n_j \in \mathcal{J}_j} e_p(u_j n_j) \right) \\ & \times \sideset{}{'}\sum_{\substack{\boldsymbol{x}\in X \\ 0\le x_i\le p-1}} e_p(-u_1 g_1(\boldsymbol{x}) - \dots - u_s g_s(\boldsymbol{x}) - t_1 x_1 - \dots - t_r x_r), \end{aligned}$$

where $\sum'$ means we ignore the poles of the g_i's when summing.

Proof. From the orthogonal relation of the exponential sum

$$\sum_{|t_i|\le (p-1)/2} e_p(t_i(m_i - x_i)) = \begin{cases} p & \text{if } x_i = m_i, \\ 0 & \text{if } x_i \ne m_i, \end{cases}$$

we sum over all possible $m_i \in \mathcal{I}_i$ to get

$$\frac{1}{p} \sum_{m_i \in \mathcal{I}_i} \sum_{|t_i|\le (p-1)/2} e_p(t_i(m_i - x_i)) = \begin{cases} 1 & \text{if } x_i \in \mathcal{I}_i, \\ 0 & \text{if } x_i \notin \mathcal{I}_i. \end{cases}$$

In the same spirit, we get

$$\frac{1}{p} \sum_{n_j \in \mathcal{J}_j} \sum_{|u_j|\le (p-1)/2} e_p(u_j(n_j - g_j(\boldsymbol{x})) = \begin{cases} 1 & \text{if } g_j(\boldsymbol{x}) \in \mathcal{J}_j, \\ 0 & \text{if } g_j(\boldsymbol{x}) \notin \mathcal{J}_j. \end{cases}$$

Therefore,

$$\frac{1}{p^{r+s}} \prod_{1\le i\le r} \prod_{1\le j\le s} \sum_{m_i\in\mathcal{I}_i} \sum_{|t_i|\le (p-1)/2} \sum_{n_j\in\mathcal{J}_j} \sum_{|u_j|\le (p-1)/2} e_p(t_i(m_i-x_i))e_p(u_j(n_j-h_j(\boldsymbol{x}))$$
$$= \begin{cases} 1 & \text{if } \boldsymbol{x}\in \mathcal{I}_1\times\cdots\times\mathcal{I}_r \text{ and } \boldsymbol{g}(\boldsymbol{x})\in \mathcal{J}_1\times\cdots\times\mathcal{J}_s, \\ 0 & \text{otherwise.} \end{cases}$$

Finally, $\mathcal{N}(X)$ is the sum of the above quantity over all possible $\boldsymbol{x}\in X$. By rearranging terms on the repeated sums we get the lemma.

□

The main term of $\mathcal{N}(X)$ corresponds to the term with all $t_i = u_j = 0$ in the above lemma, which is

$$\frac{1}{p^{r+s}} |\mathcal{I}_1|\dots|\mathcal{I}_r|\,|\mathcal{J}_1|\dots|\mathcal{J}_s|\,\#X(\mathbb{F}_p).$$

By (2.1), this is

$$\begin{aligned} \text{main term } &= \frac{1}{p^{r+s}} |\mathcal{I}_1|\dots|\mathcal{I}_r|\,|\mathcal{J}_1|\dots|\mathcal{J}_s|\,(p+O(\sqrt{p})) \\ &= \frac{1}{p^{r+s-1}} |\mathcal{I}_1|\dots|\mathcal{I}_r|\,|\mathcal{J}_1|\dots|\mathcal{J}_s| + O((r+s)\sqrt{p}). \end{aligned} \tag{2.2}$$

The following two lemmas estimate the remaining terms.

Lemma 2.4. *Let p be a large prime. For any interval $\mathcal{I}$, we have*

$$\left| \sum_{1\le |t|\le \frac{p-1}{2}} \sum_{m\in\mathcal{I}} e_p(tm) \right| \le 2p\log p.$$

Proof. Let $\mathcal{I}\cap\mathbb{Z} = \{l, l+1, \dots, l+h-1\}$, where $h = |\mathcal{I}|$. Then

$$\sum_{m\in\mathcal{I}} e_p(tm) = \begin{cases} h & \text{if } t=0, \\ \left(e^{\frac{-2\pi i t l}{p}}\right) \frac{1-e^{-2\pi i t h/p}}{1-e^{-2\pi i t/p}} & \text{if } t\neq 0. \end{cases}$$

Hence if $t\neq 0$,

$$\left| \sum_{m\in\mathcal{I}} e_p(tm) \right| \le \frac{2}{\left|1-e^{-2\pi i t/p}\right|}.$$

Since $\left|1-e^{-2\pi i t/p}\right| = 2\left|\sin(\pi t/p)\right| \ge \frac{\pi|t|}{p}$ for p large enough, we obtain the estimate

$$\left| \sum_{m\in\mathcal{I}} e_p(tm) \right| \le \frac{2p}{\pi|t|} \le \frac{p}{|t|}.$$

Finally, the lemma is obtained by summing over all t with $1\le|t|\le(p-1)/2$, using the elementary inequality

$$1+\frac{1}{2}+\cdots+\frac{1}{\frac{p-1}{2}} \le \log p.$$

□

Lemma 2.5. *If $(t_1, \dots, t_r, u_1, \dots, u_s) \neq (0, \dots, 0)$, the degree d of X is greater than 1, $1 \leq \deg(\boldsymbol{g}) < d$, and the set $\{1, x_1, \dots, x_r, g_1(\boldsymbol{x}), \dots, g_s(\boldsymbol{x})\}$ is linearly independent on X, then*

$$\left| \sum_{\substack{\boldsymbol{x} \in X \\ 0 \leq x_i \leq p-1}} e_p(-u_1 g_1(\boldsymbol{x}) - \cdots - u_s g_s(\boldsymbol{x}) - t_1 x_1 - \cdots - t_r x_r) \right| \leq d(d-1)\sqrt{p} + \frac{1}{2}d^2.$$

Proof. Apply Theorem 6 of [2] to the projective closure of X. (Note that since $1 \leq \deg(\boldsymbol{g}) < d$, the assumption of that theorem is satisfied for all large enough p.) □

Proof of Theorem 2.1. With the main term (2.2) already established, we only have to estimate other terms corresponding to nonzero $(t_1, \dots, t_r, u_1, \dots, u_s)$ in Lemma 2.3. The innermost sum for those terms is estimated uniformly by Lemma 2.5. Now group those terms according to the number of nonzero t_i and u_j, use Lemma 2.4 for nonzero t_i, u_j, and the trivial estimate $\sum_{m_i \in \mathcal{I}_i} e_p(t_i m_i) \leq p$ for $t_i = 0$ (or the equivalent for $u_j = 0$). We see that the absolute value of the remaining terms is less than or equal to

$$(2^{r+s}\log^{r+s} p + (r+s)2^{r+s-1}\log^{r+s-1} p + \binom{r+s}{2} 2^{r+s-2}\log^{r+s-2} p + \dots + 2(r+s)\log p) \times (d(d-1)\sqrt{p} + \frac{1}{2}d^2)$$

which is

$$2^{r+s} d(d-1)\sqrt{p}\log^{r+s} p + O(\sqrt{p}\log^{r+s-1} p).$$

This finishes the proof of Theorem 2.1. □

Remark 2.6. From the proof of Theorem 2.1, we see that if some of the intervals among $\mathcal{I}_i, \mathcal{J}_j$ are the full interval $[0, p)$, then we can loosen the linearly independent condition a little bit. This will be vital in our application later.

Let $\mathcal{I}_i$ correspond to the coordinate functions x_i, and $\mathcal{J}_j$ correspond to the functions $g_j(\boldsymbol{x})$. From the proof of Lemma 2.3, we see that if any of the $\mathcal{I}_i$ or $\mathcal{J}_j$ is the full interval, the exponential sum over that interval and its corresponding function can be omitted. Thus when we apply Bombieri's estimate in Lemma 2.5, we can remove the function from the set we require to be linearly independent if its corresponding interval is the full one.

As an example of how we make use of the above remark, we let $r = s$ and $\boldsymbol{g}$ to be the identity map. Then it is not necessary to restrict our range to any subset. Hence all $\mathcal{J}_j$'s are full. From the remark we only need to ensure the set $\{1, x_1, \dots, x_r\}$ is linearly independent, and this is true since the degree of X is $d > 1$. Thus we recover the uniform distribution theorem in [6], now with an explicit error term.

Corollary 2.7. *Let X be as usual, of degree $d > 1$, and $|\mathcal{I}|$ denotes the number of integers inside $\mathcal{I}$. Let*

$$\mathcal{N}'(X) = \#\{\boldsymbol{x} \in X \cap (\mathcal{I}_1 \times \cdots \times \mathcal{I}_n)\}$$

the number of points of X lying inside the hypercube $\mathcal{I}_1 \times \cdots \times \mathcal{I}_n$. If p is a large prime, then

$$\left| \mathcal{N}'(X) - \frac{|\mathcal{I}_1| \dots |\mathcal{I}_r|}{p^{r-1}} \right| \leq 2^r d(d-1)\sqrt{p}\log^r p + O(\sqrt{p}\log^{r-1} p).$$

As another application, if we do not restrict our domain, that is if all $\mathcal{I}_i$'s are full, then using Remark 2.6 we recover [14, Theorem 1] in the special case where Ω is a hypercube.

3. r-tuples of x-coordinates of a hyperelliptic curve mod p with a prescribed rational function

For the remaining of the paper, we let C be a hyperelliptic curve over $\mathbb{F}_p$ defined by the equation $y^2 = f(x)$, with $d = \deg f$. We assume f is not a square in $\overline{\mathbb{F}_p}(x)$, so that C is irreducible. We are interested in the distribution of the distances between successive x-coordinates of points on C, subjected to a restricted range of a rational function in terms of the two successive points (we will make this precise in a moment). Our approach is inspired by [3], where the distribution of the distances between successive primitive roots mod p is studied.

Let $\mathcal{H} = \{h_1, \dots, h_r\}$ be a subset of $\{1, 2, \dots, p-1\}$. To each pair of $(C, \mathcal{H})$, we define the *x-shifted curve* of C by $\mathcal{H}$, $C_{\mathcal{H}}$, to be the curve defined by the family of equations

$$\begin{aligned} y^2 &= f(x) \\ y_1^2 &= f(x+h_1) \\ &\vdots \\ y_r^2 &= f(x+h_r) \end{aligned}$$

in $\mathbb{A}_p^{r+2}$ with the $r+2$ coordinates $x, y, y_1, \dots, y_r$ (the shifted curve also appeared in [9], but the definition here is a little bit different). It is easy to see that $C_{\mathcal{H}}$ is indeed a curve.

Let S be the set of all $x \in \mathbb{F}_p$ so that there is a y with $(x, y) \in C(\mathbb{F}_p)$. From the definition of $C_{\mathcal{H}}$, it is obvious that a point on $C_{\mathcal{H}}$ corresponds to an x such that x and $x + h_i$ are all in S for all $h_i \in \mathcal{H}$.

More generally, if $\mathcal{I}$ is an interval in $[0, p)$, let $S_{\mathcal{I}}$ be the set of all x so that there is a $y \in \mathcal{I}$ with $(x, y) \in C(\mathbb{F}_p)$. Then there is a correspondence from the set of points on $C_{\mathcal{H}}$ inside the hypercube $([0, p) \times \mathcal{I}^{r+1})$ to the set of x's so that all x and $x + h_i$ are in $S_{\mathcal{I}}$ for all $h_i \in \mathcal{H}$.

Now suppose $P = (x, y)$ and $P_0 = (x_0, y_0)$ are two points on C, $g = g(P, P_0) = g(x, y, x_0, y_0)$ is a rational function between the 2 points. With respect to a point $P = (x, y)$, we define $S_{\mathcal{I},\mathcal{J},P}$ to be the set of all x_0 in $S_{\mathcal{I}}$ satisfying the extra condition $g(P, P_0) \in \mathcal{J}$, for some $P_0 = (x_0, y_0)$ on C with $y_0 \in \mathcal{I}$. If $g_i = g(P, P_i) = g(x, y, x + h_i, y_i)$ is the rational function obtained from g by putting in $P_0 = (x + h_i, y_i)$, and let $\boldsymbol{g} = (g_1, \dots, g_r)$, then $\boldsymbol{g}$ is a rational function on $C_{\mathcal{H}}$. It is clear that there is a correspondence from the set of points on $C_{\mathcal{H}}$ inside the hypercube $([0, p) \times \mathcal{I}^{r+1})$ whose image under $\boldsymbol{g}$ lie in $\mathcal{J}^r$ to the set of x's such that ($P = (x, y)$ as usual) $x + h_i$ are in $S_{\mathcal{I},\mathcal{J},P}$ for all $h_i \in \mathcal{H}$.

To simplify matters, from now on we assume that the interval $\mathcal{I} \subset [0, (p-1)/2]$, so that one x-value can only correspond to at most one y-value, and hence the

above correspondence is bijective. We define $\mathcal{N}(\mathcal{H}) = \mathcal{N}(\mathcal{H}; C, p, g, \mathcal{I}, \mathcal{J})$ to be the number of points on $C_{\mathcal{H}}$ inside the hypercube $([0,p) \times \mathcal{I}^{r+1})$ whose image under $\boldsymbol{g}$ lie in $\mathcal{J}^r$. The following lemma gives an idea of the size of $\mathcal{N}(\mathcal{H})$.

Lemma 3.1. *Let C be a hyperelliptic curve defined by $y^2 = f(x)$. Let $\mathcal{H} = \{h_1, \dots, h_r\}$, $f \in \mathbb{F}_p[x]$ of degree d, not a square in $\overline{\mathbb{F}_p}[x]$, and $g(P, P_0)$ a rational function between two points in X, of degree $\deg g < d$, and the set $\{1, g_1, \dots, g_r\}$ is linearly independent on $C_{\mathcal{H}}$. If d and r are small compared to p, then for all sufficiently large p,*

$$\left| \mathcal{N}(\mathcal{H}) - \frac{|\mathcal{I}|^{r+1} |\mathcal{J}|^r}{p^{2r}} \right| \leq 2^{3r+2} d(2^r d - 1) \sqrt{p} \log^{2r+2} p + O(\sqrt{p} \log^{2r+1} p).$$

Proof. It is easy to compute that $D = \deg C_{\mathcal{H}} = 2^r d$. Once we show that $C_{\mathcal{H}}$ is irreducible, this lemma will follow from replacing r by $r+2$, letting $s = r$, $\mathcal{I}_i = \mathcal{I}$, $\mathcal{J}_j = \mathcal{J}$ and $\boldsymbol{g} = (g_1, \dots, g_r)$ (recall that $g_i = g(P, P_i)$) in Theorem 2.1. Note that by Remark 2.6 there is no need to include the function x in the set of functions we require to be linearly independent since its corresponding interval is full.

We show the irreducibility of $C_{\mathcal{H}}$ by showing that the field

$$K = \mathbb{F}_p(x) \left[\sqrt{f(x)}, \sqrt{f(x+h_1)}, \dots, \sqrt{f(x+h_r)} \right]$$

obtained by adjoining a square root of each of the $f(x)$ and $f(x+h_i)$ is the function field of $C_{\mathcal{H}}$. The condition that r is small compared to p ensures that K is a field extension of degree 2^{r+1} over $\mathbb{F}_p(x)$. Now we proceed using induction on r.

For $r = 0$ this follows from the condition that f is not a square.

Assume that $K_{r-1} = \mathbb{F}_p(x) \left[\sqrt{f(x)}, \sqrt{f(x+h_1)}, \dots, \sqrt{f(x+h_r)} \right]$ is the function field of $C_{\mathcal{H}'}$, where $\mathcal{H}' = \mathcal{H} - h_r$. K_{r-1} is a field of degree 2^r over $\mathbb{F}_p(x)$. Let $I = \langle y^2 - f(x), y_1^2 - f(x+h_1), \dots, y_{r-1}^2 - f(x+h_{r-1}) \rangle$ be the ideal of $\mathcal{H}'$. Then we have an isomorphism

$$\frac{\mathbb{F}_p(x)[y, y_1, \dots, y_{r-1}]}{I} \xrightarrow{\sim} K_{r-1}$$

obtained by sending $y \mapsto \sqrt{f(x)}, y_i \mapsto \sqrt{f(x+h_i)}$. The induction is completed if we can prove that the map

$$\frac{K_{r-1}[y_r]}{y_r^2 - f(x+h_r)} \xrightarrow{\phi} K = K_{r-1} \left[\sqrt{f(x+h_r)} \right] \tag{3.1}$$

with $y_r \mapsto \sqrt{f(x+h_r)}$, is an isomorphism. The map ϕ is clearly surjective, and from the degrees of the fields K, K_{r-1} over $\mathbb{F}_p(x)$, we see that K is a vector space over K_{r-1} of dimension 2. Since the left hand side of (3.1) has rank at most 2 over K_{r-1}, ϕ must be an isomorphism. □

Remark 3.2. If $\mathcal{J}$ is the full interval, then by using Lemma 2.6, we can remove the assumption that the set $\{1, g_1, \dots, g_r\}$ is linearly independent on $C_{\mathcal{H}}$.

Remark 3.3. For the rest of the paper, we will assume that as $p \to \infty$, we have $d = o(p)$, $r = o(\log p / \log\log p)$, $|\mathcal{I}| \geq p / \log\log p$, and $\mathcal{J} = [\alpha p, \beta p)$ $(0 \leq \alpha < \beta \leq 1)$. It is clear that under these conditions, the proof of Lemma 3.1 works and the main term has a bigger magnitude than the error term when p is sufficiently large.

Next, if $\mathcal{A}, \mathcal{B}$ are two disjoint sets of integers, we define

$$\mathcal{N}(\mathcal{A}, \mathcal{B}) = \mathcal{N}(\mathcal{A}, \mathcal{B}; C, p, \mathcal{I}, \mathcal{J})$$

to be the number of x such that x and $x+a$ are in $S_{\mathcal{I},\mathcal{J}}$ for all $a \in \mathcal{A}$, but $x+b$ are not in $S_{\mathcal{I},\mathcal{J}}$ for any $b \in \mathcal{B}$. To estimate $\mathcal{N}(\mathcal{A}, \mathcal{B})$, we introduce the characteristic function

$$\delta(x) = \begin{cases} 1 & \text{if } x \in S_{\mathcal{I},\mathcal{J}}, \\ 0 & \text{otherwise.} \end{cases}$$

Since in our case one x can correspond to at most one y, we can write $\mathcal{N}(\mathcal{A}, \mathcal{B})$ in terms of $\delta(x)$,

$$\begin{aligned} \mathcal{N}(\mathcal{A}, \mathcal{B}) &= \sum_{x \in [0,p)} \prod_{a \in \mathcal{A}} \delta(x+a) \prod_{b \in \mathcal{B}} (1 - \delta(x+b)) \\ &= \sum_{x \in [0,p)} \prod_{a \in \mathcal{A}} \delta(x+a) \sum_{\mathcal{C} \subset \mathcal{B}} (-1)^{|\mathcal{C}|} \prod_{c \in \mathcal{C}} \delta(x+c) \\ &= \sum_{\mathcal{C} \subset \mathcal{B}} (-1)^{|\mathcal{C}|} \sum_{x \in [0,p)} \prod_{d \in \mathcal{A} \cup \mathcal{C}} \delta(x+d) \\ &= \sum_{\mathcal{C} \subset \mathcal{B}} (-1)^{|\mathcal{C}|} \mathcal{N}(\mathcal{A} \cup \mathcal{C}). \end{aligned}$$

Combining this with Lemma 3.1, which says

$$\mathcal{N}(\mathcal{H}) = \frac{|\mathcal{I}|^{|\mathcal{H}|+1} |\mathcal{J}|^{|\mathcal{H}|}}{p^{2|\mathcal{H}|}} + \theta_{\mathcal{H}} 2^{3|\mathcal{H}|+2} d(2^{|\mathcal{H}|} d - 1) \sqrt{p} \log^{2|\mathcal{H}|+2} p + O(\sqrt{p} \log^{2|\mathcal{H}|+1} p)$$

for some $|\theta_{\mathcal{H}}| \le 1$, we get the following result.

Theorem 3.4. *Let $\mathcal{A}, \mathcal{B}$ be two sets of integers distinct mod p. Then*

$$\begin{aligned} &\left| \mathcal{N}(\mathcal{A}, \mathcal{B}) - |\mathcal{I}| \left(\frac{|\mathcal{I}| \, |\mathcal{J}|}{p^2} \right)^{|\mathcal{A}|} \left(1 - \frac{|\mathcal{I}| \, |\mathcal{J}|}{p^2} \right)^{|\mathcal{B}|} \right| \\ &\quad \le 2^{3|\mathcal{A}|+4|\mathcal{B}|+1} d(2^{|\mathcal{A}|+|\mathcal{B}|} d - 1) \sqrt{p} \log^{2|\mathcal{A}|+2|\mathcal{B}|+2} p + O(\sqrt{p} \log^{2|\mathcal{A}|+2|\mathcal{B}|+1} p). \end{aligned}$$

Remark 3.5. Theorem 3.4 only depends on the cardinality of $\mathcal{A}, \mathcal{B}$ and also the number of integers in the interval $\mathcal{I}$, but not the particular elements in $\mathcal{A}, \mathcal{B}$ and the position of $\mathcal{I}, \mathcal{J}$. It is interesting to compare Theorem 3.4 with Theorem 1 in [3].

We remind the reader that we have assumed that

$$d = o(p), \qquad |\mathcal{A}|, |\mathcal{B}| = o(\log p / \log\log p) \qquad \text{and} \qquad |\mathcal{I}|, |\mathcal{J}| \ge p / \log\log p.$$

See Remark 3.3.

4. The Poisson distribution of the x-coordinates

Recall that $S_{\mathcal{I}}$ is the set of all x so that there is a $y \in \mathcal{I}$ with $(x, y) \in C$, and for $P = (x, y) \in C$, $S_{\mathcal{I},\mathcal{J},P}$ is the set of all x_0 in $S_{\mathcal{I}}$ satisfying the extra condition $g(P, P_0) \in \mathcal{J}$, for some $P_0 = (x_0, y_0)$ on C with $y_0 \in \mathcal{I}$. For $t \ge 1$ and k a non-negative integer, we define $P_k(t) = P_k(t; C, p, g, \mathcal{I}, \mathcal{J})$ to be the proportion of

$x \in S_{\mathcal{I}}$ for which the interval $(x, x+t]$ contains exactly k elements in $S_{\mathcal{I},\mathcal{J},P}$ with $P = (x, y)$ as usual. Note that by Corollary 2.7, the cardinality of $S_{\mathcal{I}}$ satisfies

$$||S_{\mathcal{I}}| - |\mathcal{I}|| \leq 4d(d-1)\sqrt{p}\log^2 p + O(\sqrt{p}\log p),$$

or equivalently, for some $|\theta| \leq 1$,

$$\begin{aligned} |S_{\mathcal{I}}| &= |\mathcal{I}| + 4\theta d(d-1)\sqrt{p}\log^2 p + O(\sqrt{p}\log p) \\ &= |\mathcal{I}| \left(1 + \frac{4\theta d(d-1)\sqrt{p}\log^2 p}{|\mathcal{I}|} + O(\log p/\,|\mathcal{I}|)\right). \end{aligned} \tag{4.1}$$

Next, we write $P_k(t)$ in terms of the quantities $\mathcal{N}(\mathcal{A}, \mathcal{B})$.

$$P_k(t) = \frac{1}{|S_{\mathcal{I}}|} \sum_{\substack{\mathcal{C} \subset \{1,\ldots,[t]\} \\ |\mathcal{C}| = k}} \mathcal{N}(\mathcal{C}, \overline{\mathcal{C}}),$$

where $\overline{\mathcal{C}} = \{1, \ldots, [t]\} - \mathcal{C}$.

For $t = o(\log p/\log\log p)$, $k \leq t$, $|\mathcal{I}| \geq p/\log\log p$, and $\mathcal{J} = [\alpha p, \beta p)$, we can apply Theorem 3.4 and (4.1) to obtain

$$\begin{aligned} P_k(t) = &\left(1 + \frac{4\theta d(d-1)\sqrt{p}\log^2 p}{|\mathcal{I}|} + O(\log p/\,|\mathcal{I}|)\right)^{-1} \\ &\times \left(\sum_{\substack{\mathcal{C} \subset \{1,\ldots,[t]\} \\ |\mathcal{C}| = k}} \left(\frac{|\mathcal{I}|\,|\mathcal{J}|}{p^2}\right)^{|\mathcal{C}|} \left(1 - \frac{|\mathcal{I}|\,|\mathcal{J}|}{p^2}\right)^{|\overline{\mathcal{C}}|} + E\right) \end{aligned}$$

with

$$E = \frac{1}{|\mathcal{I}|}\theta' 2^{4[t]+1} d(2^{[t]}d - 1)\sqrt{p}\log^{2[t]+2} p + O(\sqrt{p}\log^{2[t]+1} p),\ |\theta'| \leq 1.$$

This simplifies to

$$P_k(t) = \binom{[t]}{k} \left(\frac{|\mathcal{I}|\,|\mathcal{J}|}{p^2}\right)^k \left(1 - \frac{|\mathcal{I}|\,|\mathcal{J}|}{p^2}\right)^{[t]-k} + O(p^{-1/2}\log^{2[t]+3} p), \tag{4.2}$$

where the constant in $O(p^{-1/2}\log^{2[t]+3} p)$ can be taken as $2^{4[t]+1}d(2^{[t]}d - 1)$.

Suppose now p goes to infinity, while $\lambda = t\,|\mathcal{I}|\,/p$ remains fixed (so that t goes to infinity as $p \to \infty$, and automatically $|\mathcal{I}| = o(p)$). Note that the condition $|\mathcal{I}| \geq p/\log\log p$ guarantees that $t = O(\log\log p)$ (so it is certainly $o(\log p/\log\log p)$) and hence it guarantees that our formula works throughout the limiting process. We also have $|\mathcal{J}|\,/p \to \beta - \alpha$. As $p \to \infty$, the error term is at most $O(p^{-1/2+\delta})$ for any $\delta > 0$. Thus (4.2) shows that asymptotically $P_k(t)$ has a Poisson distribution with parameter $\lambda(\beta - \alpha)$:

$$P_k(t) \sim e^{-\lambda(\beta-\alpha)} \frac{(\lambda(\beta-\alpha))^k}{k!}$$

for any non-negative integer k. More precisely, we have

Theorem 4.1. *Let k be a non-negative integer. Suppose $t = O(\log\log p)$, $|\mathcal{I}| \geq p(\log\log p)^2/\log p$, $|\mathcal{I}| = o(p)$ and $\mathcal{J} = [\alpha p, \beta p)$. Set $\lambda = t\,|\mathcal{I}|\,/p$, then as p goes to*

infinity, we have

$$P_k(t) = e^{-\lambda(\beta-\alpha)} \frac{((\beta-\alpha)\lambda)^k}{k!} e^{O((1+k+\lambda(\beta-\alpha))|\mathcal{I}|/p)} \left[1 + O\left(\frac{k^2\,|\mathcal{I}|}{\lambda p(\beta-\alpha)}\right)\right] + O(p^{\frac{-1}{2}+\delta})$$

for any $\delta > 0$.

For any real number $\lambda > 0$, define $\mu(\lambda, \alpha, \beta) = \mu(\lambda, \alpha, \beta; C, p, \mathcal{I})$ as in (1.1) in the introduction. It is easy to see that this equals $P_0(t)$, with $t = \lambda p/\,|\mathcal{I}|$. Thus by putting $k = 0$ in Theorem 4.1, we obtain

Corollary 4.2. *For any* $\delta > 0$*, under the conditions of Theorem 4.1, we have*

$$\mu(\lambda, \alpha, \beta) = e^{-\lambda(\beta-\alpha)} e^{O((1+\lambda(\beta-\alpha))/\log\log p)} + O(p^{\frac{-1}{2}+\delta}).$$

Therefore, if we let $p \to \infty$*, then*

$$\lim_{p\to\infty} \mu(\lambda, \alpha, \beta) = e^{-\lambda(\beta-\alpha)}.$$

Moreover, the convergence is uniform on compact subsets of $[0, \infty)$.

Proof. The only thing we still need to prove is the uniform convergence on compact subsets. Unlike the primitive root case considered in [3], this comes for free, since if p is large enough, *every* p satisfies the conditions of Theorem 4.1. □

An important special case is obtained by letting $\mathcal{J}$ to be the full interval $[0, p)$, and $g(P, P_0) = x(P)$, the x-coordinates of the base point. Then if we let $\mu(\lambda) = \mu(\lambda, 0, 1)$, this is the proportion of consecutive x-coordinates in $S_{\mathcal{I}}$ whose distances are greater than $\lambda p/\,|\mathcal{I}|$. We get the following direct analogue of the primitive root case considered in [3].

Corollary 4.3. *For any* $\delta > 0$*, under the conditions of Theorem 4.1, and the additional condition that* $\mathcal{J}$ *is the full interval* $[0, p)$*, then as* p *tends to infinity, the distribution of the number of* x*-coordinates in* $S_{\mathcal{I}}$ *in short intervals approaches a Poisson distribution with parameter* λ*:*

$$P_k(t) \sim e^{-\lambda} \frac{\lambda^k}{k!}.$$

Also, the distribution of the distances between consecutive x*-coordinates satisfies*

$$\mu(\lambda) = e^{-\lambda} e^{O((1+\lambda)/\log\log p)} + O(p^{\frac{-1}{2}+\delta}).$$

In particular, as $p \to \infty$*,*

$$\lim_{p\to\infty} \mu(\lambda) = e^{-\lambda}.$$

Remark 4.4. It is not absolutely necessary to consider $(x, y) \in C$ to lie in the rectangle $[0, p) \times \mathcal{I}$. For example, by a linear change of variable, we can consider any parallelogram which has length p (in the x-direction), as long as the y-coordinates of the rectangle lie totally inside $[0, (p-1)/2]$, and the width (in the y-direction) satisfies the requirement for $|\mathcal{I}|$.

For more general domains with piecewise smooth boundaries, one can apply the Lipschitz's principle on the number of integer points [5]. In that case, the error term will be much weaker, but the limiting process is still valid.

Remark 4.5. It may also be interesting to see what happens if $\mathcal{I}$ is too big, say $\mathcal{I} = [0, (p-1)/2]$. From (4.2), which is still valid for this big $\mathcal{I}$, we have

$$P_k(t) = \binom{[t]}{k} \left(\frac{|\mathcal{I}|\,|\mathcal{J}|}{p^2}\right)^k \left(1 - \frac{|\mathcal{I}|\,|\mathcal{J}|}{p^2}\right)^{[t]-k} + O(p^{-1/2}\log^{2[t]+3} p).$$

As $p \to \infty$ with $\lambda = t\,|\mathcal{I}|\,/p$ kept constant, this just gives

$$P_k(t) \to \binom{[t]}{k} \left(\frac{1}{2}(\beta-\alpha)\right)^k \left(1 - \frac{1}{2}(\beta-\alpha)\right)^{t-k}$$

and hence

$$P_0(t) \to (1 - 1/2(\beta-\alpha))^t \sim (1 - 1/2(\beta-\alpha))^{2\lambda},$$

which is never close to something like $e^{-\lambda}$. The reason is that as $p \to \infty$, t does not go to infinity accordingly, but stays more or less constant.

5. An application

As an application of our results, we consider the distribution of x-coordinates of points on an elliptic curve in a rectangle, and the distortion of the distribution by the group law. More precisely, let E be an elliptic curve defined by $y^2 = x^3 + ax + b$ over $\mathbb{F}_p$. Let $\mathcal{I} \subset [0, (p-1)/2]$ be an interval satisfying $|\mathcal{I}| \le p/\log\log p$. We order the points $P_i = (x_i, y_i)$ of C in the rectangle $[0, p) \times \mathcal{I}$ according to the size of the x-coordinates: $0 \le x_1 < \cdots < x_m < p$.

We are interested in the distribution of the distances between consecutive x-coordinates $x_{i+1} - x_i$, where $x_{m+1} = x_1 + p$. By Corollary 4.3, the proportion of distances at least λ times the asymptotic average $p/\,|\mathcal{I}|$ satisfies

$$\lim_{p\to\infty} \frac{\#\{i : 1 \le i \le m, x_{i+1} - x_i \ge \lambda p/\,|\mathcal{I}|\}}{m} = e^{-\lambda}.$$

We now look at how the group law of the elliptic curve may distort the above distribution. Recall that (see for example [12]) if $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ are two points in C with $x \ne x_0$, the group law on C reads

$$\begin{aligned} x(P_1 + P_2) &= \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \\ y(P_1 + P_2) &= -\frac{y_2 - y_1}{x_2 - x_1} x(P_1 + P_2) - \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}, \\ -P_1 &= (x, -y). \end{aligned} \tag{5.1}$$

Fix an interval $\mathcal{J} = [\alpha p, \beta p)$. We want to see the proportion of consecutive points P_i, P_{i+1} (in the above sense) for which the distances between their x-coordinates are large, and also the x-coordinates of their differences $x(P_{i+1} - P_i)$ lie inside $\mathcal{J}$. From the group law (5.1) above, we have

$$x(P_{i+1} - P_i) = \left(\frac{y_{i+1} + y_i}{x_{i+1} - x_i}\right)^2 - x_i - x_{i+1}.$$

Suppose $P = (x, y)$ is a base point, and $P_i = (x + h_i, y_i)$. Take $g_i(P, P_i) = x(P_i - P) = \left(\frac{y_i + y}{h_i}\right)^2 - 2x - h_i$ to be the difference map. Before applying Corollary 4.2, we need the following lemma.

Lemma 5.1. *The set $\{1, g_1, \ldots, g_r\}$ is linearly independent on $C_{\mathcal{H}}$ for any $\mathcal{H} = \{h_1, \ldots, h_r\}$.*

Proof. Fix any $\mathcal{H} = \{h_1, \ldots, h_r\}$. Suppose there are constants $c_0, c_1, \ldots, c_r \in \mathbb{F}_p$ such that

$$c_0 + c_1 g_1 + \ldots + c_r g_r = 0$$

on $C_{\mathcal{H}}$, i.e.

$$c_0 + c_1((h_1^{-1})^2(y_1+y)^2 - 2x - h_1) + \ldots + c_r((h_r^{-1})^2(y_r+y)^2 - 2x - h_r) = 0 \tag{5.2}$$

on $C_{\mathcal{H}}$. Expand this equation and notice that due to the defining equations of $C_{\mathcal{H}}$, all terms with y^2 and y_i^2 can be transformed into terms involving x only. This gives

$$2c_1(h_1^{-1})^2 y y_1 + \ldots + 2c_r(h_r^{-1})^2 y y_r + P(x) = 0,$$

where $P(x)$ is a polynomial in x with coefficients in $\mathbb{F}_p$. Hence $c_i(h_i^{-1})^2 = 0$ for all $i = 1, 2, \ldots, r$. This implies $c_i = 0$ for such i since $h_i \neq 0$. By (5.2), we also have $c_0 = 0$. This completes the proof of the lemma. □

Now we can apply Corollary 4.2 to get

$$\lim_{p\to\infty} \frac{\#\{1 \le i \le m : x_{i+1} - x_i \ge \lambda p/\,|\mathcal{I}| \text{ and } x(P_{i+1} - P_i) \in [\alpha p, \beta p)\}}{m} = e^{-(\beta-\alpha)\lambda}.$$

Thus under the extra condition about the difference map between consecutive points, the distribution of the distance $x_{i+1} - x_i$ is still of the same type, but with a different constant. Note that the new distribution only depends on the length of the interval $[\alpha p, \beta p)$, but not on the group law. That is, we get similar results for any two-point rational function $g(P, P_0)$.

Acknowledgements. The authors wish to thank the referee for the suggestion of many improvements to this paper.

References

[1] Y. Aubry and M. Perret, *A Weil theorem for singular curves*, Arithmetic, geometry and coding theory (Luminy, 1993), de Gruyter, Berlin, 1996, pp. 1–7.

[2] E. Bombieri, *On exponential sums in finite fields*, Amer. J. Math. **88** (1966), no. 1, 71–105.

[3] C. Cobeli and A. Zaharescu, *On the distribution of primitive roots mod p*, Acta Arith. **83** (1998), no. 2, 143–153.

[4] ———, *On the distribution of the $\mathbf{F}_p$-points on an affine curve in r dimensions*, Acta Arith. **99** (2001), no. 4, 321–329.

[5] H. Davenport, *On a principle of Lipschitz*, J. London Math. Soc. **26** (1951), 179–183.

[6] M. Fujiwara, *Distribution of rational points on varieties over finite fields*, Mathematika **35** (1988), no. 2, 155–171.

[7] A. Granville, I. E. Shparlinski, and A. Zaharescu, *On the distribution of rational functions along a curve over $\mathbb{F}_p$ and residue races*, J. Number Theory **112** (2005), no. 2, 216–237.

[8] W. Luo, *Rational points on complete intersections over $\mathbf{F}_p$*, Internat. Math. Res. Notices (1999), no. 16, 901–907.

[9] K.-H. Mak and A. Zaharescu, *The distribution of values of short hybrid exponential sums on curves over finite fields*, Math. Res. Lett. **18** (2011), no. 1, 155–174.

[10] G. Myerson, *The distribution of rational points on varieties defined over a finite field*, Mathematika **28** (1981), no. 2, 153–159 (1982).

[11] I. E. Shparlinskiĭ and Alexei N. Skorobogatov, *Exponential sums and rational points on complete intersections*, Mathematika **37** (1990), no. 2, 201–208.

[12] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

[13] A. N. Skorobogatov, *Exponential sums, the geometry of hyperplane sections, and some Diophantine problems*, Israel J. Math. **80** (1992), no. 3, 359–379.

[14] M. Vajaitu and A. Zaharescu, *Distribution of values of rational maps on the $\mathbf{F}_p$-points on an affine curve*, Monatsh. Math. **136** (2002), no. 1, 81–86.

[15] A. Zaharescu, *The distribution of the values of a rational function modulo a big prime*, J. Théor. Nombres Bordeaux **15** (2003).

Department of Mathematics, University of Illinois at Urbana-Champaign, 273 Altgeld Hall, MC-382, 1409 W. Green Street, Urbana, Illinois 61801, USA
E-mail address: mak4@illinois.edu

Department of Mathematics, University of Illinois at Urbana-Champaign, 273 Altgeld Hall, MC-382, 1409 W. Green Street, Urbana, Illinois 61801, USA
E-mail address: zaharesc@math.uiuc.edu